Forum for American Leadership

How the Federal Government Should Fight Digital Identity Fraud

May 1, 2024

The Top Line: Implementing zero trust principles is cybersecurity best practice. The first pillar of zero trust is strong digital identity—that means determining the identity of a user before they can access a service or application to ensure they have the right authorization. Lack of strong digital identity verification was a major vector for COVID relief fraud. The Biden Administration started strong on zero trust and digital identity policy, but succumbed to activist pressure related to concern over government surveillance, civil liberties infringement, and potentially disproportionate racial outcomes inhibiting implementation. The result left America and taxpayer-funded relief less secure. The time to reinvigorate and restructure digital identity approaches is now.

The Forum for American Leadership's Technology and National Security Innovation Working Group outlines what the U.S. government is getting right and wrong on digital identity and prudent next steps to scale digital identity as a cybersecurity best practice.

DEFINITIONS

- **Zero Trust** assumes a network is compromised and enforces security controls to stop an attacker from moving laterally or escalating privileges to get higher accesses.
- **Digital identity** is the confirmation that an online user is who they assert they are and have access to the applications they assert that they do.
- **Identity proofing**, the most politically sensitive aspect of digital identity, establishes that a subject is who they claim to be. For example, matching a person to their driver's license or unlocking your smartphone with your fingerprint.
- **Multi-factor authentication (MFA)** requires presenting two or more factors (password, biometric, SMS-push code) to verify identity.
- **Login.gov** is a government employee-coded digital identity solution built by GSA.

THE STATE-OF-PLAY

- Cybersecurity is crucial to the national economy because buyer and seller trust in online applications increases the flow of commerce. The federal government is rapidly digitizing and as part of this effort is implementing a zero trust approach to security based on industry best practice. In May 2021, President Biden issued Executive Order 14028, "Improving the Nation's Cybersecurity," directing federal agencies to implement a zero trust architecture.
    - OMB guidance followed in January 2022 defining the five pillars of zero trust, the first of which is digital identity. This was a welcome, early development.
    - By March 2023, Pillar 4.5 of the *National Cybersecurity Strategy* called on the government to support development of a digital identity ecosystem, but fell short of endorsing key efforts to establish digital identities, like the state-government roll-out of mobile driver licenses (mDL) taking place in four initial states and

under review in over 20, potentially missing a key opportunity to endorse advances in the digital identity ecosystem.
    - Following pressure from civil liberties activists and internal White House turf wars over cybersecurity roles and missions and the collection, use, and retention of biometrics records, the follow-on July 2023 *National Cybersecurity Strategy Implementation Plan* (NCSIP) omitted any mention of the digital identity pillar.
- Beginning in 2022, President Biden acknowledged that rampant pandemic fraud driven by identity theft enabled multi-billion dollar fraud from several COVID-related relief benefits in two successive State of the Union speeches. The White House promised an Executive Order on preventing identity theft in public benefits. But two years on amid massive fraud documented by both the Secret Service (USSS) and the Special Inspector General for Pandemic Recovery (SIGPR), scandal and IG investigations, and pressure from the ACLU and under-represented racial groups over the collection, use, and retention of biometrics by the government–namely facial recognition—no such EO has been promulgated.
    - Critics of the Administration's inaction have also been harassed.
        - In January 2022, Blake Hall, an Army veteran, entrepreneur, and CEO of remote identity proofing vendor ID.me—Login.gov's leading commercial competitor—estimated that COVID unemployment relief fraud may have reached $400 billion, generating media attention and embarrassing the Biden Administration.
        - Three months later, the then-Democratic majority of the House Oversight Committee launched an investigation of ID.me lasting over a year, which some saw as retribution for Hall's criticism of the Administration's handling of digital identity security.
        - The USSS itself has since estimated pandemic fraud as high as $100 billion.
- NIST Special Publication 800-63 defines digital identity guidelines for the public sector.
    - Draft revisions were due in 2021. After a lengthy delay amidst White House domestic policy pressure, NIST revised the standard to conform to President Executive Order 13985 on diversity, equity, and inclusion (DEI).
    - In NIST's draft, elevated assurance levels will no longer require biometric proofs like facial recognition due concerns over government surveillance from civil society activists like the ACLU and disparate outcomes of facial recognition for trans and individuals of color. In other words, under the new standard, an identity proofing capability can *claim* a higher level of security and assurance without actually *incorporating* higher security methods, like facial recognition.
    - NIST's change to its digital identity standard would also grant *ex post facto* higher security status to Login.gov, a legacy IT system from the Obama-era.
- A creation of the Obama Administration, Login.gov was developed by GSA's Office of Technology Transformation Services (TTS) and was formalized on President Obama's last day in office in January 2017.
    - TTS is a federal office that codes government software and is often critiqued for duplicating capabilities available for license in the commercial sector.
        - For example:

        - Notify.gov duplicates capabilities available from Twilio or MessageBird.
        - Login.gov duplicates capabilities available from ID.me, 1Kosmos, Microsoft, and other identity vendors.
    - According to a recently separated GSA official, Login.gov was premised on an ideological mistrust of the American private sector.
    - In autumn 2021, one GSA program management office awarded another GSA program management office a $187 million Technology Modernization Fund (TMF) grant for Login.gov—the largest single TMF award ever. The total all-in development costs of Login.gov are unknown.
- The GSA Office of the Inspector General (OIG) investigated Login.gov in 2022 and found that while TTS claimed that Login.gov offered a higher assurance level for identity proofing associated with use of biometrics based on NIST 800-63, its actual capabilities fell short of the standard, thereby misleading its federal agency customers.
    - Congress, for its part, held an oversight hearing in spring 2023 and issued several letters, which have yet to be answered by the GAO, GSA, and other addressees.
- Both the House and the Senate are moving forward to advance *Federal Information Security Modernization Act* (*FISMA*) reform legislation aimed at reauthorizing and expanding a statute that currently provides Login.gov a *de jure* monopoly in government digital identity.
    - The Senate provision led by Sens. Peters (D-MI) and Wyden (D-OR) would strengthen Login.gov's monopoly, while reform legislation championed by Reps. Comer (R-KY) and Sessions (R-TX) would curb the government monopoly paving the path for commercial solutions.

IMPLICATIONS AND NEXT STEPS

- Compromised credentials and identity-related attacks constitute 80% of all cyber attacks.
    - For example, both the 2019 Capital One breach and this summer's Microsoft hack by China's Storm-0558 threat actor that exposed the emails of senior government officials relied on compromised credentials.
- The *National Cybersecurity Strategy* frames digital identity purely around citizen services, while remaining silent on the need to implement digital identity controls like MFA across the federal workforce and critical infrastructure owners and operators.
    - The Biden Administration should have accomplished this expansion of strong digital identity efforts within its first term instead of investing resources in a government homebrew solution duplicative of commercial capabilities; a new Republican Administration should begin this effort on day one.
- In a time of great power competition, the U.S. government should increase its ties and connections with Silicon Valley innovators by making the U.S. government a better market for commercial products and better buyer of widely available technologies across the board. This starts with the government not being a subsidized competitor to commercial innovation.

    - For more ideas on how this can be accomplished in the DOD space, see the Forum for American Leadership (FAL) paper, "How DoD Can Modernize Faster," available here.
    - In addition, the 50+ government-run software factories, like TTS, should be required to do a review of whether a desired software capability can be bought rather than being custom-built.
- NIST is widely and deeply well-respected for its professionalism and impartiality; in order to maintain this status, the current and future Administrations should seek to avoid efforts aiming at influencing on NIST standards, particularly when such efforts are aimed at appeasing activists and advancing domestic social policies should not find purchase in NIST standards.

Conclusion: The Biden Administration's early steps on zero trust and digital identity were promising but now show signs of being derailed. In the last year of this Administration or the first year of the next, the government should:

- Issue an *Identity Theft EO* that requires strong biometric-enabled identity proofing to access government services online and clears away policy barriers to acquiring commercial digital identity solutions;
- Reign-in TTS and require the government to determine whether it would be more efficient and cost-effective to buy, rather than build capabilities that already exist in the commercial sector;
- Ignore the activists calling for NIST to decouple the use of biometrics in digital identity proofing from higher security ratings and keep NIST apolitical; and
- Issue policy guidance to encourage states to issue mobile driver licenses while taking reasonable steps and precautions to reassure that government use of digital identity will not lead to federal snooping, tracking, or surveillance of U.S. citizens.

This paper is a product of the Forum for American Leadership's Technology and National Security Innovation Working Group.

The Forum for American Leadership (FAL) is a non-profit organization that presents expert analysis and national security recommendations to policymakers in Congress and the Executive Branch.